Sur le nombre de points d'une courbe sur un corps fini ; application aux codes correcteurs d'erreurs

Marc PERRET

Résumé — Le nombre A(q) est la limite supérieure du nombre maximum de points d'une courbe définie sur $\mathbf{F}_q$ divisé par le genre. J.-P. Serre a montré l'existence d'une constante $c > 0$ telle que $A(q) > c \log q$. Sa méthode, liée à l'existence de tours infinies de corps de classes de Hilbert, peut donner de meilleurs résultats ; on donne ici de nouvelles minorations de A(q) pour certaines valeurs de q, et on en déduit l'existence de nouvelles familles de codes sur $\mathbf{F}_q$ dépassant la borne de Varshamov-Gilbert.

On the number of points of a curve over a finite field ; application to error-correcting codes

Abstract — *The number* A(q) *is the superior limit of the maximum number of points of a curve defined over* $\mathbf{F}_q$ *divided by the genus. It has been shown by J.-P. Serre that* $A(q) > c \log q$, *where c is a positive constant. His method, depending on the existence of infinite towers of Hilbert-class fields, can give better results ; we give here some new lower bounds of* A(q) *for some* q, *and we deduce from these the existence of new families of codes defined over* $\mathbf{F}_q$ *exceeding the Varshamov-Gilbert bound.*

Abridged English Version. Let p be a prime number, and q a power of p. If $g \in \mathbf{N}^*$, let N(g,q) be the maximum number of rational points over $\mathbf{F}_q$ of an irreducible algebraic smooth curve of genus g defined over $\mathbf{F}_q$. We define $A(q) = \limsup_{g \to \infty} \frac{N(g,q)}{g}$. In this note, we give a lower bound of A(q) for certain values of q.

THEOREM 1. *Let* l *be a prime number,* $k \in \mathbf{N}^*$, *and suppose that q is a primitive k-root of unity in* $\mathbf{F}_l$. *Then :*

$$A(q^l) \geq \frac{\sqrt{(l(q-1)) - 2l}}{l-1} \quad \textit{if } k = 1,$$

and

$$A(q^k) \geq \frac{\sqrt{(l(q-1)) - 2l}}{l-1} \quad \textit{if } k \geq 2.$$

Sketch of the proof. If K is a function field of one variable over $\mathbf{F}_q$, whose exact constant field is $\mathbf{F}_q$, and if S is a non empty finite set of places of K of degree one, we define K_a as the maximum unramified abelian extension of K of exponent dividing l, in which the places of S split completely. Let S_a be the set of places of K_a dividing the places of S. By iteration, we obtain a tower of fields with $K_0 = K$ and $K_n = (K_{n-1})_a$ for $n \geq 1$, and for each field K_n, a non empty finite set of places : $S_0 = S$, $S_n = (S_{n-1})_a$ for $n \geq 1$. The tower (K_n,S_n) is called the *Hilbert* l-*class-field tower* of (K,S). In order to prove theorem 1,the first step is to find a condition on (K,S) for the tower (K_n,S_n) to be infinite ; the second step is then to construct a pair (K,S) satisfying this condition, from which we deduce the desired lower bound.

1) First step. Let $K^\infty = \tilde{\bigcup}_{n \geq 0} K_n$, $G = \mathrm{Gal}(K^\infty/K)$, and $G_1 = \mathrm{Gal}(K_1/K)$. G and G_1 are pro-l-groups, so we can define as in [7] the number $d = d(G) = d(G_1)$.

Note présentée par Jean-Pierre Serre

PROPOSITION 1. *If* $d+|S| \le d^2/4$, *then the extension* K^{∞}/K *is infinite*.

2) Second step. Let $k_0 = \mathbf{F}_q(T)$, and suppose $q \equiv 1 \pmod{l}$. Let A, B be two disjoint parts of $\mathbf{F}_q$, $a = |A|$, $b = |B|$, and consider the fields $K_0 = k_0(U)$, where $U^l = \prod_{\alpha \in A} (T - \alpha)$, and $K_\alpha = k_0(U_\alpha)$, where $U_\alpha{}^l = T - \alpha$, for $\alpha \in A$. Suppose that for all $\alpha \in A$ and $\beta \in B$, $\beta - \alpha$ is a l-power in $\mathbf{F}_q$, and denote by S_0 the set of places of K_0 dividing the places $(T - \beta)$ of k_0, for $\beta \in B$. Then $|S0| = lb$.

PROPOSITION 2. *Assume* $q \equiv 1 \pmod{l}$ *and* $(|A|, l) = 1$. *The fields* K_α, *where* α *runs over all the elements of A except one , are independent unramified cyclic extensions of degree* l *of* K_0, *in which the elements of* S_0 *split completely*. *Moreover,* $d(G) = d(G_1) \ge |A| - 1$.

3) Last step. The following proposition results easily from propositions 1 and 2 :

PROPOSITION 3. *Let* l *be a prime number such that* $q \equiv 1 \pmod{l}$. *If one can find two disjoint parts A and B of* $\mathbf{F}_q$, *satisfying :*

a) $B - A \subset \mathbf{F}_q^{\infty l}$,

b) $a + lb - 1 \le (a-1)^2/4$,

c) $(a, l) = 1$, *then*

$$A(q) \ge \frac{2bl}{(a-1)(l-1)} \quad .$$

Theorem 1 follows from proposition 3, where {A, B} is a partition of $\mathbf{F}_q$, and from computing the smaller value of a (resp. the greater value of b), satisfying both relations $a + lb - 1 \le (a-1)^2/4$ and $a + b = q$. Then one use the Hurwitz genus formula.

Finally, we explain how to deduce from a theorem of Tsfasman and theorem 1 the existence of new families of codes exceeding the Varshamov-Gilbert bound.

I. INTRODUCTION.

Soient p un nombre premier et q une puissance de p. Si g est un entier, on désigne par N(g, q) le nombre maximum de points rationnels sur le corps fini $\mathbf{F}_q$ à q éléments d'une courbe lisse de genre g définie sur $\mathbf{F}_q$, et on pose

$$A(q) = \limsup_{g \to \infty} \frac{N(g,q)}{g} \quad .$$

Drinfeld et Vladut ont montré dans [2] que $A(q) \le \sqrt{q} - 1$. D'autre part, Tsfasman, Vladut et Zink ont montré dans [9] que les courbes de Shimura sur $\mathbf{F}_{q^2}$ atteignent cette borne, ainsi $A(q) = \sqrt{q} - 1$ si q est un carré. En outre, Serre (cf. [8]) a montré que $A(q) > c \log q$ pour tout q, où c est une constante positive non nulle.

La détermination de A(q) n'est pas seulement intéressante en elle-même : elle permet de montrer que dans certains cas, il existe une famille de codes sur $\mathbf{F}_q$ dépassant la borne de Varshamov-Gilbert (voir IV). Par exemple l'égalité $A(q^2) = q - 1$ montre que si $q \geq 7$, alors il existe une famille de codes sur $\mathbf{F}_{q^2}$ dépassant la borne de Varshamov-Gilbert (cf [2], [9], [6]).

Nous obtenons ici une minoration de A(q) pour certaines valeurs de q, que nous utilisons pour obtenir des codes dépassant la borne de Varshamov-Gilbert. On procède comme suit : le corps des fonctions d'une courbe sur $\mathbf{F}_q$ est une extension de degré de transcendance 1 de $\mathbf{F}_q$, et un point rationnel sur $\mathbf{F}_q$ de la courbe s'identifie à une place de degré 1 de son corps de fonctions. Soit donc K_0 un corps de fonctions d'une variable sur $\mathbf{F}_q$, et S_0 un ensemble fini non vide de places de K_0 ; on va considérer, pour un nombre premier l fixé à l'avance, la l -*tour de corps de classes de Hilbert de* (K_0, S_0), et donner un critère, qui repose sur un théorème de Golod et Shafarevich, pour que cette tour soit infinie. On choisira ensuite (K_0, S_0) répondant à ce critère, tel que les étages de sa l-tour aient beaucoup de points par rapport au genre ; on en déduira alors une minoration de A(q). La méthode qui suit permettant de choisir le couple (K_0, S_0) est due à J.-P. Serre, que je remercie pour les améliorations qu'il a apportées aux résultats obtenus initialement.

II. LA METHODE DE SERRE.

1. Tours de corps de classes de Hilbert. Soit K une extension de degré de transcendance 1 de $\mathbf{F}_q$. On suppose que le corps des constantes de K est égal à $\mathbf{F}_q$. Soient l un nombre premier, et S un ensemble fini non vide de places de K, dont l'une au moins est de degré premier à l. On considère la plus grande extension abélienne K_a de K, d'exposant l, non ramifiée, où les places de S sont totalement décomposées. On note S_a l'ensemble des places de K_a au-dessus de S. En itérant cette construction, on obtient une suite d'extensions

$$K_0 = K, K_n = (K_{n-1})_a \text{ pour } n \geq 1,$$

et pour chaque corps K_n, un ensemble fini non vide de places : $S_0 = S$, $S_n = (S_{n-1})_a$ pour $n \geq 1$. Posons

$$K^\infty = \underset{n \geq 0}{\approx} K_n,$$

$$G = \mathrm{Gal}(K^\infty/K), \text{ et } G_1 = \mathrm{Gal}(K_1/K).$$

La suite $(K_n, S_n)_{n \geq 0}$ est appelée la l -*tour de corps de classes de Hilbert au-dessus de* (K, S). Le problème consiste à trouver un critère permettant d'affirmer que l'extension K^∞/K est infinie.
Les groupes G et G_1 sont des pro-l-groupes, et G_1 est même un l - groupe fini. On note d(G) (resp. $d(G_1)$) le nombre minimum de générateurs de G (resp. G_1), et r(G) le nombre minimum de relations entre d(G) générateurs de G. Ces deux nombres ont une interprétation cohomologique (cf. [7]). Puisque G_1 est le plus grand quotient de G de type (l, …, l), il est clair que $d(G_1) = d(G)$. Vinberg et Gaschütz ont montré que si G est fini et si $d(G) \geq 1$, alors $r(G) > d^2(G)/4$, améliorant ainsi un théorème de Golod et Shafarevich ; pour une démonstration, voir [1]. De plus, on peut étendre aux corps de fonctions algébriques à une variable sur $\mathbf{F}_q$ un résultat d'Iwasawa (voir [3]) sur les corps

de nombres pour voir que si G est fini, alors $r(G) - d(G) \leq |S| + \delta$, avec $\delta = 0$ si $l \mid q - 1$, et $\delta = -1$ sinon. On peut donc conclure, en posant $d = d(G_1) = d(G)$:

THEOREME 1. *Si* $d + |S| + \delta \leq d^2/4$, *et si* $d \geq 1$, *alors l'extension* K^∞/K *est infinie*.

2. Procédé de construction. On pose $k_0 = \mathbf{F}_q(T)$. On suppose que $q \equiv 1 \pmod{l}$. Soient A et B deux parties non vides et disjointes de $\mathbf{F}_q$. On considère le corps

$$K_0 = k_0(U), \qquad \text{ou} \qquad U^l = \prod_{\alpha \in A} (T - \alpha) ,$$

ainsi que les corps

$$K_\alpha = k_0(U_\alpha), \text{ ou } U_\alpha{}^l = T - \alpha \ , \text{ pour } \alpha \in A .$$

On pose

$$\mathbf{F}_q^{\infty l} = \{x^l ; x \in \mathbf{F}_q^\infty \} ;$$

on suppose que pour tout $\alpha \in A$ et tout $\beta \in B$, $\beta - \alpha$ est une puissance l-ième dans $\mathbf{F}_q$, ce que l'on note :

$$B - A \subset \mathbf{F}_q^{\infty l} .$$

On note enfin S_0 l'ensemble des places de K_0 au dessus des places $(T - \beta)$ de k_0, pour tout $\beta \in B$; on a $/S_0/ = l/B/$; toute place de S_0 est de degré 1.

PROPOSITION 1. *Supposons* $q \equiv 1 \pmod{l}$ *et* $(|A|, l) = 1$. *Les corps* K_α , *où* α *parcourt tous les éléments de A sauf un, sont des extensions cycliques de degré* l *de* K_0, *indépendantes et non ramifiées, où les éléments de* S_0 *se décomposent totalement. De plus :*

$$d(G) = d(G_1) \geq |A| - 1.$$

3. Minoration de $A(q)$. La méthode suivie permet de montrer le théorème suivant.

THEOREME 2. *Soit* l *un nombre premier, tel que* $q \equiv 1 \pmod{l}$. *Si on peut trouver deux parties disjointes* A *et B de* $\mathbf{F}_q$, *telles que* $|A| = a \geq 2$, $|B| = b \geq 1$, *et de plus :*

a) $B - A \subset \mathbf{F}_q^{\infty l}$,

b) $a + lb - 1 \leq (a-1)^2/4$,

c) $(a, l) = 1$,

alors

$$A(q) \geq \frac{2bl}{(a-1)(l-1)} \quad .$$

En particulier :

EQ $\o(_Q;\s\up4(l))$, *on a*

$$A(Q) \geq \frac{\sqrt{(l(q-1)) - 2l}}{l-1} \ ,$$

pour peu que $q > 4l + 1$.

Le corollaire 1 se déduit facilement du théorème 2 en prenant pour A et B une partition de $\mathbf{F}_q$. On calcule alors la plus petite valeur de a (resp.la plus grande valeur de b) vérifiant la condition b) du théorème 2, ainsi que la relation a + b = q. Afin d'appliquer le théorème 2, il faut s'assurer que (a, l) = 1, ce qui n'est pas toujours vrai pour cette valeur de a. Il faut donc augmenter a (resp.diminuer b) d'une unité. Le théorème 2 donne alors une minoration compliquée de A(q), elle-même minorée par celle du corollaire. La condition $q > 4l + 1$ implique les conditions $a \geq 2$ et $b \geq 1$.

Il reste à montrer le théorème 2. A cette fin on construit comme au n°2 le couple (K_0,S_0) à partir des ensembles A et B. La condition b) de l'énoncé permet d'affirmer, via la proposition 1 et le théorème 1, que la l-tour de corps de classes de Hilbert au-dessus de (K_0, S_0) est infinie. Ainsi :

$$A(q) \geq \lim_{n \to \infty} \{\text{nombre de places de degré 1 de } K_n\} / g_n \geq \lim_{n \to \infty} \frac{|S_n|}{g_n} \quad .$$

Or, l'extension K_n/K_0 est non ramifiée, donc $2g_n - 2 = [K_n : K_0] (2g_0 - 2)$; par suite

$$A(q) \geq \lim_{n \to \infty} ([K_n : K_0]|S_0|) / ([K_n : K_0] (g_0 - 1) + 1) = |S_0| / (g_0 - 1) = lb / (g_0 - 1),$$

puisque $\lim_{n \to \infty} [K_n : K_0] = + \infty$. La formule de Hurwitz appliquée à K_0/k_0 où $k_0 = \mathbf{F}_q(T)$, montre que

$$g_0 - 1 = \frac{(a + 1) (l - 1)}{2} - 1 < \frac{(a - 1) (l - 1)}{2} \quad .$$

Cela résulte de ce que l'indice de ramification e_α d'une place $(T - \alpha)$, où $\alpha \in A$, divise $[K_0 : k_0] = l$; ces places sont donc totalement ramifiées. De même, l'hypothèse (a, l) = 1 implique que l'indice de ramification e_∞ de la place à l'infini est égal à l ; les ramifications sont modérées car l'hypothèse $q \equiv 1 \pmod{l}$ implique (l, q) = 1 ; cela montre le théorème 2.

III. LE THEOREME PRINCIPAL.

Soit l un nombre premier.

THEOREME 3. *Supposons* $q > 4l + 1$. *Soient k un entier non nul et q une racine primitive k-ième de l'unité dans* $\mathbf{F}_l$. *Si* $k = 1$ (i.e. si $q \equiv 1 \pmod{l}$), *alors*

$$A(q^l) \geq \frac{\sqrt{(l(q - 1)) - 2l}}{l - 1} \quad ;$$

si $k \geq 2$, *alors*

$$A(q^k) \geq \frac{\sqrt{(l(q - 1)) - 2l}}{l - 1} \quad .$$

Par exemple : 1) Si q est impair, $q > 9$, la méthode donne $A(q^2) \geq \sqrt{2}\sqrt{q-1} - 4$, ce qui est moins bon que la borne $A(q^2) = \sqrt{q} - 1$ de Tsfasman, Vladut et Zink citée dans [9].

2) Si $q \equiv 1 \pmod{3}$, ou si $q \equiv 2$ ou $4 \pmod{7}$, alors:

$$A(q^3) \geq \frac{\sqrt{3}}{2} \sqrt{q-1} - 3 \qquad \text{pour } q > 13.$$

Signalons que Zink a montré que dans le cas où q = p est premier, on a $A(p^3) \geq 2 \frac{p^2-1}{p+2}$ (cf. [10]) .

3) De même, si $q \equiv 1 \pmod 5$, alors :

$$A(q^5) \geq \frac{\sqrt{5}}{4}\sqrt{q-1} - \frac{5}{2} \qquad \text{pour } q > 21.$$

Le théorème 3 découle du corollaire 1 et des deux remarques suivantes:
1) si $q \equiv 1 \pmod l$, tous les éléments de $\mathbf{F}_q$ sont des puissances l-ièmes dans $\mathbf{F}_{q^l}$.
2) si $(l, q-1) = 1$, tous les éléments de $\mathbf{F}_q$ sont des puissances l-ièmes dans $\mathbf{F}_q$, donc aussi dans $\mathbf{F}_{q^k}$.
L'hypothèse q racine primitive k-ième de l'unité dans $\mathbf{F}_l$ signifie que $q^k \equiv 1 \pmod l$, ce qui est une hypothèse primordiale dans le corollaire 1.

IV. APPLICATION AUX CODES CORRECTEURS D'ERREURS.

On renvoie à [4] et [5] pour les notations et la terminologie sur les codes correcteurs d'erreurs sur $\mathbf{F}_q$, ainsi qu'à [6] pour un exposé plus complet de ce qui suit.Tsfasman a montré le théorème suivant : l'intersection de la droite $x + y = 1 - 1/A(q)$ avec le carré $[0,1]^2$ est incluse dans le domaine des codes. Puisque la courbe de Varshamov-Gilbert est convexe, décroissante, et que sa tangente de pente -1 est la droite d'équation

$$x + y = 1 - \log_q \textbf{ Erreur !},$$

le théorème de Tsfasman montre qu'il y a des codes dépassant la borne de Varshamov-Gilbert dès que $\frac{1}{A(q)} < \log_q \frac{2q-1}{q}$. On déduit de cette relation et du théorème 3 :

THEOREME 4. *Sous les hypothèses et notations du théorème 3, si*

$$\frac{l-1}{\sqrt{(l\,(q-1)) - 2l}} < \log_{q^l} \frac{2q^l - 1}{q^l} \quad ,$$

(resp.,si

$$\frac{l-1}{\sqrt{(l\,(q-1)) - 2l}} < \log_{q^k} \frac{2q^k - 1}{q^k} \quad),$$

alors il existe une famille de codes sur $\mathbf{F}_{q^l}$ (resp.$\mathbf{F}_{q^k}$), dépassant la borne de Varshamov-Gilbert .

Par exemple, si q est impair, la construction précédente montre l'existence de familles de codes dépassant la borne de Varshamov-Gilbert pour $q \geq 191$, ce qui est moins bon que le résultat annoncé dans [9]. De même, si $q \geq 1657$, et si $q \equiv 1 \pmod 3$, ou si $q \equiv 2$ ou $4 \pmod 7$, cette construction donne de telles familles sur $\mathbf{F}_{q^3}$; si $q \geq 16981$ et si $q \equiv 1 \pmod 5$, on a la même conclusion sur $\mathbf{F}_{q^5}$.

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] J.W.S. CASSELS et A. FRÖHLICH, *Algebraic Number Theory,* Academic Press, 1967.

[2] V.G. DRINFELD et S.G., VLADUT, Number of points of an algebraic curve, *Funktsional'nyi Analiz i Ego Prilozheniya* **17** (1983), p. 68-69 ; =*Functional Analysis* **17** (1983), p. 53-54.

[3] K. IWASAWA, A note on the group of units of an algebraic number field, *Journ. Math. Pures et Appl.* **35** (1956), p. 189-192.

[4] G. LACHAUD, Les codes géométriques de Goppa, Séminaire Bourbaki 1984/1985, exp. n° 641, *Astérisque* **133-134** (1986), p. 189-207.

[5] Yu. I. MANIN et S.G. VLADUT, Codes linéaires et courbes modulaires, *Itogi Nauki i Tekhniki* **25** (1984), p. 209-257 ; trad. angl., *J. Soviet Math.* **30** (1985), p. 2611-2643 ; trad. franç., *Pub. Math. Univ. Pierre et Marie Curie*, n°72, 91 p.

[6] M.PERRET,Families of codes exceeding the Varshamov-Gilbert bound,*à paraitre aux actes du colloque "3 journées sur le codage",1988,université de Toulon,* Lecture Notes in Computer Sciences, Springer.

[7] J.-P. SERRE,*Cohomologie galoisienne*, Lecture Notes in Math. 5, Springer, Berlin, 1965.

[8] J.-P. SERRE, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C. R. Acad. Sc. Paris* **296** (1983), p. 397-402 ; = *Œuvres*, n° 128, vol. III, p. 658-663.

[9] M.A. TSFASMAN, S.G. VLADUT et T. ZINK, Modular Curves, Shimura Curves, and Goppa Codes, better than Varshamov-Gilbert bound, *Math. Nachr.* **109** (1982), p. 21-28.

[10] T.ZINK, Degeneration of Shimura surfaces and a problem in coding theory, *Fundamentals of computation theory, (cottbus,1985)*, p. 503 - 511, Lecture Notes in Computer Sciences, 199, Springer, New York, (1985).

Équipe CNRS
"Arithmétique & Théorie de l'Information"
C.I.R.M.
Luminy Case 916
13 288 Marseille CEDEX 9